UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/598,509	05/16/2007	Richard Michael Wyn Harran	GB920040005US1	6651

25259   7590   11/10/2008

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
RESEARCH TRIANGLE PARK, NC 27709

EXAMINER
VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
11/10/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

RSWIPLAW@us.ibm.com

	Application No.	Applicant(s)
Office Action Summary	10/598,509	HARRAN ET AL.
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 May 2007*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 39-54* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 39-54* is/are rejected.

7)☒ Claim(s) *1,39 and 50* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 September 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date *9/1/06*.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/598509 filed on 5/16/07 is

presented for examination by the examiner.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C.

119(a)-(d). The certified copy has been received.

Claim Objections

Claims 1, 39, and 50 are objected to because of the following informalities:

As per claims 1, 39 and 50, there is a lack of antecedent basis for "the previously

idle communications link".

As per claim 39, the phrase "said first and a second entity" would be clearer if it

were written as "said first entity and a second entity". Having said with the antecedent

better solidifies its relationship.

Specification

The disclosure is objected to because of the following informalities: lacks

appropriate US section headings.

Appropriate correction is required.

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR
      DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A
      COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
      (1) Field of the Invention.
      (2) Description of Related Art including information disclosed under 37
      CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A
      "Sequence Listing" is required on paper if the application discloses a
      nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if
      the required "Sequence Listing" is not submitted as an electronic
      document on compact disc).

Title

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:
Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 50-54 are rejected under 35 U.S.C. 101 as directed to non-statutory subject matter of software, per se. The language of claim should include computer "readable" media and state that the program is stored on a computer readable media, causing a computer to execute in the active voice. Claims 51-54 are likewise rejected for failing to remedy the above reason for rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 39, 44, and 50 are rejected under 35 U.S.C. 102(e) as being anticipated by USP 6,795,555 to Parisien et al., hereinafter Parisien.

As per claim 1, Parisien teaches a method for facilitating secure data communications using a secret key for encrypting data flowing between first and second entities over a communications link (Fig. 1), the method comprising: determining that the communications link has been idle (col. 4, lines 37-38); determining that there is data to flow over the previously idle communications link (col. 2, lines 5-10); and responsive to determining that there is data to flow over the previously idle communications link, initiating generation of a new secret key, the new secret key for encrypting data sent between the first and the second entities over the communications link (col. 5, lines 30-35).

As per claim 39, Parisien teaches a method performed at a first entity for facilitating secure data communications by using a secret key for encrypting data flowing between said first and a second entity over a communications link, the method comprising the steps of:

determining that the communications link has been idle (col. 4, lines 37-38);

determining whether data is available for flow over the previously idle communications link (col. 2, lines 5-10); and

in response to a determination that data is available, initiating generation of a new secret key for use in encoding at least part of the available data before it flows onto the communications link (col. 5, lines 30-35).

As per claim 44, Parisien teaches an apparatus for facilitating secure data communications by using a secret key to encrypt data flowing over a communications link between the apparatus and a remote system, said apparatus comprising:

a data detector for determining whether the communications link has been idle

and whether data is now available for flow to the remote system over the

communications link (col. 4, lines 37-38);

key generation logic responsive to determinations that the communications link

has been idle and there is data now available for flow to the remote system to initiate

generation of a new secret key for use in encoding at least part of the available data

before it flows onto the communications link (col. 5, lines 30-35).

As per claim 50, Parisien teaches a program product comprising a computer

usable media embodying program (col. 7, line 30) instructions which, when executed in

a computer, results in the computer facilitating secure data communications with a

remote system by using a secret key for encrypting data flowing between

the computer and the remote system over a communications link by:

determining that the communications link has been idle (col. 4, lines 37-38);

determining whether data is available for flow over the previously idle

communications link (col. 2, lines 5-10; and

in response to a determination that data is available, initiating generation of a

new secret key for use in encoding at least part of the available data before it flows onto

the communications link (col. 5, lines 30-35.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 40-43, 45-49, and 51-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parisien in view of EP 0999673 to Mamros et al., hereinafter Mamros.

As per claim 40, Parisien is silent in disclosing the step of determining that the link has been idle for at least a predetermined period of time and the step of initiating generation of a new secret key is performed only if the communications link is found to have been idle for at least the predetermined period of time. Mamros teaches changing keys after a predetermined time (0032). Parisien does teach that only when the communication is idle do the keys get updated. Mamros teaches the notion of measuring the amount of time between key updates so avoid unnecessary overhead (0032). Thus is it important not to needlessly generate new keys close too close to one another. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Mamros into the teachings of Parisien because it would alleviate too frequent key updates and therefore save processing time and computation overhead.

As per claim 41, Parisien is silent in disclosing determining whether the amount of data sent over the communications link since the last generation of a secret key exceeds a predetermined amount threshold; and if the amount of data sent exceeds the

predetermined amount threshold, initiating generation of a new secret key. Mamros teaches determining whether the amount of data sent over the communications link since the last generation of a secret key exceeds a predetermined amount threshold; and if the amount of data sent exceeds the predetermined amount threshold, initiating generation of a new secret key (0032). It is well known in the art that the longer you use a key the more susceptible it becomes to attach. One of ordinary skill knows this and knows that is why you change keys frequently. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate Mamros' teaching into the system of Parisien. Updating the key after a transmission threshold lowers the chance of the key being discovered by an attacker.

As per claim 42, Parisien is silent in disclosing sending a heartbeat message to the second entity only if it is determined that the link has been idle has been idle for at least the predetermined period of time and that there is no data available for flow over the communications link; and monitoring the communications link for receipt of an acknowledgement from the second entity. Mamros teaches sending a heartbeat message to the second entity only if it is determined that the link has been idle has been idle for at least the predetermined period of time and that there is no data available for flow over the communications link; and monitoring the communications link for receipt of an acknowledgement from the second entity (0038). Mamros teaching is simply a means to prevent premature session ending by sending heartbeat [keep-alive] message between sender and receiver. This method is well known in the art. It is obvious to apply known techniques to known methods which yield predictable results. Therefore

the claim would have been obvious because heartbeat messages were recognized as parts of the ordinary capabilities of one skill in the art at the time of the invention.

As per claim 43, Parisien is silent in disclosing the additional step terminating the communications link with the second entity if no acknowledgement is received from the second entity within a predetermined period of time. Mamros teaches the additional step terminating the communications link with the second entity if no acknowledgement is received from the second entity within a predetermined period of time (0039). Examiner supplies the same rationale for combining Mamros and Parisien as recited in the previous rejection. The use of a heartbeat is to know the other party is still available. It would be obvious to terminate the session if the heartbeat is not acknowledged.

As per claim 45, Parisien is silent in disclosing the step of determining that the link has been idle for at least a predetermined period of time and the step of initiating generation of a new secret key is performed only if the communications link is found to have been idle for at least the predetermined period of time. Mamros teaches changing keys after a predetermined time (0032). Parisien does teach that only when the communication is idle do the keys get updated. Mamros teaches the notion of measuring the amount of time between key updates so avoid unnecessary overhead (0032). Thus is it important not to needlessly generate new keys close too close to one another. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Mamros into the teachings of

Parisien because it would alleviate too frequent key updates and therefore save
processing time and computation overhead.

As per claim 46, Parisien is silent in disclosing determining whether the amount
of data sent over the communications link since the last generation of a secret key
exceeds a predetermined amount threshold; and if the amount of data sent exceeds the
predetermined amount threshold, initiating generation of a new secret key. Mamros
teaches determining whether the amount of data sent over the communications link
since the last generation of a secret key exceeds a predetermined amount threshold;
and if the amount of data sent exceeds the predetermined amount threshold, initiating
generation of a new secret key (0032). It is well known in the art that the longer you use
a key the more susceptible it becomes to attach. One of ordinary skill knows this and
knows that is why you change keys frequently. Therefore it would have been obvious to
one of ordinary skill in the art at the time of the invention to incorporate Mamros'
teaching into the system of Parisien. Updating the key after a transmission threshold
lowers the chance of the key being discovered by an attacker.

As per claims 47 and 48, Parisien is silent in disclosing sending a heartbeat
message to the second entity only if it is determined that the link has been idle has been
idle for at least the predetermined period of time and that there is no data available for
flow over the communications link; and monitoring the communications link for receipt of
an acknowledgement from the second entity. Mamros teaches sending a heartbeat
message to the second entity only if it is determined that the link has been idle has been
idle for at least the predetermined period of time and that there is no data available for

flow over the communications link; and monitoring the communications link for receipt of

an acknowledgement from the second entity (0038). Mamros teaching is simply a

means to prevent premature session ending by sending heartbeat [keep-alive] message

between sender and receiver. This method is well known in the art. It is obvious to

apply known techniques to known methods which yield predictable results. Therefore

the claim would have been obvious because heartbeat messages were recognized as

parts of the ordinary capabilities of one skill in the art at the time of the invention.

As per claim 49, Parisien is silent in disclosing the additional step terminating the

communications link with the second entity if no acknowledgement is received from the

second entity within a predetermined period of time. Mamros teaches the additional

step terminating the communications link with the second entity if no acknowledgement

is received from the second entity within a predetermined period of time (0039).

Examiner supplies the same rationale for combining Mamros and Parisien as recited in

the previous rejection. The use of a heartbeat is to know the other party is still

available. It would be obvious to terminate the session if the heartbeat is not

acknowledged.

As per claim 51, Parisien is silent in disclosing the step of determining that the

link has been idle for at least a predetermined period of time and the step of initiating

generation of a new secret key is performed only if the communications link is found to

have been idle for at least the predetermined period of time. Mamros teaches changing

keys after a predetermined time (0032). Parisien does teach that only when the

communication is idle do the keys get updated. Mamros teaches the notion of

measuring the amount of time between key updates so avoid unnecessary overhead

(0032). Thus is it important not to needlessly generate new keys close too close to one

another. Therefore it would have been obvious to one of ordinary skill in the art at the

time of the invention to incorporate the teachings of Mamros into the teachings of

Parisien because it would alleviate too frequent key updates and therefore save

processing time and computation overhead.

As per claim 52, Parisien is silent in disclosing determining whether the amount

of data sent over the communications link since the last generation of a secret key

exceeds a predetermined amount threshold; and if the amount of data sent exceeds the

predetermined amount threshold, initiating generation of a new secret key. Mamros

teaches determining whether the amount of data sent over the communications link

since the last generation of a secret key exceeds a predetermined amount threshold;

and if the amount of data sent exceeds the predetermined amount threshold, initiating

generation of a new secret key (0032). It is well known in the art that the longer you use

a key the more susceptible it becomes to attach. One of ordinary skill knows this and

knows that is why you change keys frequently. Therefore it would have been obvious to

one of ordinary skill in the art at the time of the invention to incorporate Mamros'

teaching into the system of Parisien. Updating the key after a transmission threshold

lowers the chance of the key being discovered by an attacker.

As per claim 53, Parisien is silent in disclosing sending a heartbeat message to

the second entity only if it is determined that the link has been idle has been idle for at

least the predetermined period of time and that there is no data available for flow over

the communications link; and monitoring the communications link for receipt of an

acknowledgement from the second entity. Mamros teaches sending a heartbeat

message to the second entity only if it is determined that the link has been idle has been

idle for at least the predetermined period of time and that there is no data available for

flow over the communications link; and monitoring the communications link for receipt of

an acknowledgement from the second entity (0038). Mamros teaching is simply a

means to prevent premature session ending by sending heartbeat [keep-alive] message

between sender and receiver. This method is well known in the art. It is obvious to

apply known techniques to known methods which yield predictable results. Therefore

the claim would have been obvious because heartbeat messages were recognized as

parts of the ordinary capabilities of one skill in the art at the time of the invention.

As per claim 54, Parisien is silent in disclosing the additional step terminating the

communications link with the second entity if no acknowledgement is received from the

second entity within a predetermined period of time. Mamros teaches the additional

step terminating the communications link with the second entity if no acknowledgement

is received from the second entity within a predetermined period of time (0039).

Examiner supplies the same rationale for combining Mamros and Parisien as recited in

the previous rejection. The use of a heartbeat is to know the other party is still

available. It would be obvious to terminate the session if the heartbeat is not

acknowledged.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure is listed on the enclosed PTO-892 form.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is

(571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am

- 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Syed   Zia/

Primary Examiner, Art Unit 2431